サザンクロスルータシステム「ＡＲ４１５Ｓ」
ソフトウェアリリースノート
Version 2.9.1-20

Ver.2.9.1-20

下記のとおり機能追加、機能改善が行われました。

１．本バージョンで追加された機能

ファームウェアバージョン2.9.1-17 から2.9.1-20 へのバージョンアップにおいて、以下の機能が追加されました。

1.1 ダイナミックDNS クライアント機能

固定のIP アドレスが割り当てられなくても特定のドメイン名を利用できる、ダイナミックDNS をサポートします。この機能は、ISP より割り当てられたIP アドレスに変更があった場合などに、インターネット上に存在するダイナミックDNS サーバーに対し通知し、DNS データベースを更新します。
この機能により、ダイナミックDNS サーバーが常に最新の情報を保持でき、またサーバーに登録されたドメインから接続したいルーターのIP アドレスを検索できるようになるため、固定IP アドレスを持たないルーターへのアクセスが可能です。
これに伴い、CREATE/SET ISAKMP POLICY および CREATE/SET IPSEC POLICY コマンドのPEER パラメータをドメインで指定できるようになり、固定のIP アドレスが割り当てられていない拠点同士でのインターネットVPN が可能になります。

本製品のダイナミックDNS クライアント機能は、Dynamic Network Services 社が提供するダイナミックDNS サービス DynDNS.com（http://www.dyndns.com/）のDynamic DNS Free サービスのみに対応しています。

1.2 タグ付きフレームのブリッジ機能

ブリッジ対象フレームに対し、VLAN タグ（IEEE 802.1Q）を付けたまま送出できる機能が追加されました。L2TP を使用したリモートブリッジでも使用可能です。

1.3 VID に基づいたリモートブリッジ機能（タグVLAN-to-WAN ブリッジング）

リモートブリッジ設定時にVLAN タグ（IEEE 802.1Q）のVID に基づいたブリッジングが可能になりました。
複数VLAN（または単一VLAN）設定時にVLAN タグ（IEEE 802.1Q）をチェックし、VIDやタグの有無によりパケットの通過または破棄を行うリモートブリッジ設定が可能です。

1.4 ポート認証

スイッチポート単位、Ethernet インターフェース (eth) でLAN 上のユーザーや機器を認証する、ポート認証をサポートします。認証に成功したユーザー、機器の通信を許可します。また、認証に成功したユーザー、機器を特定のVLAN にアサインすることも可能です。また、Supplicant MAC 機能に対応し、特定の送信元MAC アドレスを持つ機器を常に認証済み/ 非認証のSupplicant として登録することが可能です。

ポート認証方式として、IEEE 802.1X 認証方式/MAC アドレスベース認証方式をサポートします。

○ 802.1X 認証

802.1X 認証は、EAP (Extensible Authentication Protocol) パケットを使用し、ユーザー単位の認証を行います。Authenticator、またはSupplicant として設定可能です。

802.1X 認証モジュールが現在サポートしているEAP 認証方式は以下のとおりです。

・Authenticator： EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP、EAPOTP (MD4/MD5)

・Supplicant： EAP-MD5、EAP-OTP (MD4/MD5)

○ MAC アドレスベース認証

機器の送信元MAC アドレスに基づいて機器単位で認証を行います。Authenticator 設定が可能です。

1.5 IPv6 マルチキャスト

IPv6 マルチキャストルーティング機能として以下の機能をサポートします。

○ MLDv1

MLDv1 (RFC2710、Multicast Listener Discovery (MLD) for IPv6) をサポートします。

MLD (Multicast Listener Discovery：マルチキャスト受信者探索) は、LAN 上のIPv6 ルーターがIPv6 ノードとメッセージを交換しあい、LAN 上にどのマルチキャストグループの受信希望者 (メンバー) がいるかを把握するためのプロトコルです。MLDは、IPv4 におけるIGMPv2 (Internet Group Management Protocol v2) と同等の機能です。

○ PIM

PIM （ Protocol Independent Multicast PIM-SM: draft-ietf-pim-sm-v2-new-05 、 PIM-DM: draft-ietf-pim-dm-new-v2-01) をサポートします。PIM (ProtocolIndependent Multicast) は、ユニキャスト用のルーティングプロトコル (EIGRP やOSPF など) から独立 (Independent) した、マルチキャスト用のルーティングプロトコルです。

PIM には PIM-DM （Protocol Independent Multicast - Dense Mode）と PIM-SM （Protocol Independent Multicast - Sparse Mode) があり、本製品は両方をサポートしています。PIM の基本動作はIPv4 と同じです。

1.6 MLD プロキシー

本機能はホストからのMLDv1/v2 パケットを上位のルーターに転送する機能です。

1.7 SNMPv3

セキュリティーと遠隔管理方法について拡張されたSNMPv3 をサポートします。

1.8 ファイアウォールセッション数の制限（リミットルール）

ファイアウォールセッション数の制限が可能です。
本製品はファイアウォールセッションを作成する際、すべてのリミットルールをチェックし、もし、対象となる通信を行う端末のセッション数が超過する場合、新たなセッションを作成しません。

1.9 LAC（L2TP Access Concentrator）機能

LAC（L2TP Access Concentrator）としての動作をサポートします。

1.10 新規サポートコマンドの追加

以下の機能に新規コマンドを追加しました。詳細はコマンドリファレンス（アライドテレシス社ＨＰ：http://www.allied-telesis.co.jp/support/list/router/ar415s/docs/index.html）を参照してください。

- ○ 運用・管理/ 記憶装置とファイルシステム
- ○ 運用・管理/ ログ
- ○ 運用・管理/ ターミナルサービス
- ○ インターフェース/ スイッチポート
- ○ PPP/PPPoE AC
- ○ IP
- ○ IPv6
- ○ IP マルチキャスト/IGMP
- ○ IP マルチキャスト/PIM
- ○ ファイアウォール
- ○ ファイアウォール/UPnP
- ○ VRRP
- ○ DHCP サーバー
- ○ L2TP
- ○ IPsec

2 本バージョンで仕様変更された機能

ファームウェアバージョン2.9.1-17 から2.9.1-20 へのバージョンアップにおいて、以下の仕様変更が行われました。

2.1 Ethernet/VLAN インターフェースのリンクアップ･ダウン時のログ

Ethernet/VLAN インターフェースのリンクアップ･ダウン時のログが記録されるようになりました。

2.2 MSS クランプ（書き換え）機能の拡張

MSS 調整機能はPPPoE 上でIP ＋ TCP のパケットに対してのみ行われていましたが、IPsec通信（PPPoE 上ではIP ＋ ESP）に対してもMSS 調整が行われるようになりました。

2.3 経路選択時の優先度変更機能の追加

経路制御プロトコルによって学習した経路の優先度（preference）の変更が可能になりました。

3 本バージョンで修正された項目

ファームウェアバージョン2.9.1-17 から2.9.1-20 へのバージョンアップにおいて、以下の項目が修正されました。

3.1 モジュールトリガーを作成する際に、SCRIPT パラメーターを複数設定しようとしてもエラーとなっていましたが、これを修正しました。

3.2 SSH 機能を使用する場合、SSH 通信にて受信した1584 バイト以上の暗号化データを処理する際に、リブートが発生しておりましたが、これを修正しました。

3.3 Unnumbered PPP インターフェースで、TTL=1 を持つICMP パケットを受信した場合、その応答パケットの送信元IP アドレスとして0.0.0.0 を使用していましたが、ローカルIP インターフェースが設定されている場合はそのIP アドレス、設定されていない場合は、ICMP パケットの転送先インターフェースのIP アドレスを使用するように修正しました。

3.4 ICMPv6 Packet Too Big メッセージを受信した際、そのメッセージによって通知されたMTU の値を、メモリー上の設定に動的に反映していましたが、これを反映しないように修正しました。

3.5 ルーター通知（RA）パケットの送信が無効のときに、受信したルーター通知パケットのCur Hop Limit フィールドの値が本製品に設定されている値と異なる場合、本製品の設定内容を書き換えてしまっていましたが、書き換えないように修正しました。

3.6 データ長が1445 Byte から1452 Byte のフラグメント化されたIPv6 PING パケットをVLAN インターフェースで受信した時に応答できませんでしたが、これを修正しました。

3.7 IPv6 フィルター機能において、フィルター対象をプロトコル番号で指定してもフィルターが正しく動作

しないことがありましたが、これを修正しました。

3.8 PUBLIC 側でマルチキャストパケットを破棄した場合、PRIVATE 側での破棄としてファイアウォールのログに記録されていましたが、これを修正しました。

3.9 異なるファイアウォールセッションで同一のTCP ポートが使用されてしまう、または同一のファイアウォールセッションで異なるTCP ポートが使用されてしまう場合がありましたが、これを修正しました。

3.10 DELETE FIREWALL コマンドでNAT=ENAPT の設定を削除することができませんでしたが、これを修正しました。

3.11 ファイアウォールにおいて、RST パケットを受信してファイアウォールセッションを切断した後、RST パケットを転送する際に、シーケンス番号またはACK 番号を不正な値で送信する場合がありましたが、これを修正しました。

3.12 PPP インターフェースに動的にIP アドレスを割り当てる設定の場合、PPP インターフェースにIP アドレスが割り当てられる前にIPsec ポリシーが作成されると、IPsecポリシーのローカルIP アドレスにLAN 側IP アドレスが設定されていましたが、正しくWAN 側のIP アドレスが設定されるように修正しました。

3.13 動的にIP アドレスを割り当てるPPP インターフェースがリンクダウンし、IPsec モジュールとISAKMP モジュールが無効になった状態でPPP インターフェースのみ再度リンクアップすると、IPsec ポリシーのローカルIP アドレスに不正なアドレス0.1.0.1が設定されていましたが、これを修正しました。

3.14 ISAKMP ポリシーのPEER パラメータにIPv6 のアドレスを設定する際に、本来であればIP アドレスしか設定できないはずが、プレフィックスまで設定できてしまっていましたが、これを修正しました。

3.15 IPsec ポリシーにてNAT-Traversal（NAT-T）を有効に設定した際、ESP パケットのTOS 値がランダムな値に設定されていましたが、これを修正しました。

3.16 IPv6 の IPsec VPN にて、セレクターにANY を指定すると、IKE フェーズ2（Quickモード）時に、ペイロードにIPV4_ADDR_SUBNET を含むパケットを送出していましたが、これをIPV6_ADDR_SUBNET に修正しました。

4 本バージョンでの制限事項・注意事項

ファームウェアバージョン2.9.1-20 には、以下の制限事項や注意事項があります。

4.1 認証サーバー

RADIUS サーバーを複数登録している場合、最初に登録したRADIUS サーバーに対してのみ、SET RADIUS コマンドのRETRANSMITCOUNT パラメーターが正しく動作しません。最初のRADIUS サーバーへの再送回数のみ、RETRANSMITCOUNT の指定値よりも1 回少なくなります。本現象は802.1x 認証を使用した場合のみ発生します。

4.2 ポート認証

○ DISABLE PORTAUTH コマンドで、PORTAUTH パラメーターに8021x を指定すると、EAP Success パケットを送信してしまいます。

○ RESET ETH コマンドによってEthernet インターフェースを初期化しても、認証状態は初期化されません。

○ 802.1x 認証済みのクライアントがログオフした場合、ログオフしたクライアントのMAC アドレスがフォワーディングデータベース (FDB) に保持されたままになります。

○ ENABLE/SET PORTAUTH PORT コマンドのSERVERTIMEOUT パラメーターが正しく動作しません。これは、SET RADIUS コマンドのTIMEOUT パラメーターとRETRANSMITCOUNT パラメーターの設定が優先されているためです。SET RADIUS コマンドで TIMEOUT × (RETRANSMITCOUNT + 1) の値を SERVERTIMEOUT より大きく設定した場合は、SERVERTIMEOUT の設定が正しく機能します。

4.3 ブリッジング

ポート1 がタグ付きパケットのブリッジングの対象となるVLAN に所属し、そのVLAN にIPアドレスが設定されている場合、ポート1 からVLAN のIP アドレス宛の通信をしようとすると、 ルーターがARP に応答せず、通信ができません。これはポート1 でのみ発生し、他のポートでは発生しません。

4.4 ダイナミックDNS

○ ダイナミックDNS のアップデートで、以下の2つのケースにおいて、アップデートは再送されません。

・本製品からのTCP SYN パケットに対して、ダイナミックDNS サーバーからのSYN ACK パケットが返って来ない場合

・本製品からのTCP SYN パケットに対して、ICMP Host Unreachable メッセージが返される場合

○ ダイナミックDNS のアップデート (HTTP GET) に対する応答として、ダイナミックDNS (HTTP) サーバーから特定のエラーコード (404 Not Found) を受信すると、SHOW DDNS コマンドのSuggested

actions の項目にHTML タグの一部が表示されることがあります。

4.5 IPv6

○ RIPng 経路を利用してIPv6 マルチキャスト通信を行っている場合、経路が無効（メトリック値が16）になっても、しばらくその経路を利用して通信を行います。

○ ガーベージコレクションタイマーが動作中のRIPng 経路は、新しいメトリック値を持つ経路情報を受信しても、タイマーが満了するまで経路情報を更新しません。

4.6 DHCPv6 サーバー

○ DHCPv6 サーバーで認証機能を使用した場合、ADD DHCP6 KEY コマンドのSTRICTパラメーターが動作しません。

○ ADD DHCP6 POLICY コマンドでDHCPv6 サーバーの設定を変更しても、サーバーからReconfigure メッセージが送信されません。ADD DHCP6 POLICY コマンドの実行後、さらにSET DHCP6 POLICY コマンドを実行してください。これにより、Reconfigure メッセージが送信されます。

5 取扱説明書・コマンドリファレンスの誤記訂正

取扱説明書（613-000666 Rev.B）・コマンドリファレンス（613-000667 Rev.C）の誤記訂正です。

5.1 VLAN 数の制限

「コマンドリファレンス」/「VLAN」

34 番目と37 番目に設定したVLAN が正常に動作しません。このため、デフォルトVLAN を含めたサポートVLAN 数は16 となります。

5.2 WAN ポート仕様

「取扱説明書」135 ページ

取扱説明書に記載の製品仕様について、以下のように訂正してお詫びします。

A.7 製品仕様/ ハードウェア/ インターフェース/WAN ポート

［誤］10BASE-T/100BASE-TX × 1（オートネゴシエーション、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定、常にMDI/MDI-X 自動切替）

［正］10BASE-T/100BASE-TX × 1（オートネゴシエーション時MDI/MDI-X 自動切替、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定時はMDI 固定）